The Office of the National Coordinator for
Health Information Technology

Security Risk Assessment Tool
Overview

ONC Web Event

April 29th, 2014

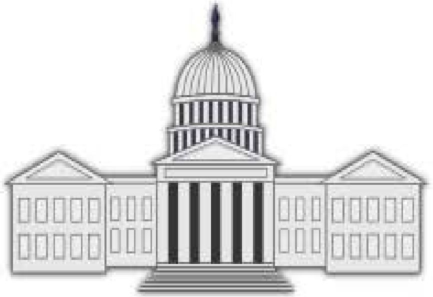
Laura Rosas, JD, MPH
Senior Advisor
Office of the Chief Privacy Officer

HealthIT.gov

Privacy and Security:
A Shared Responsibility

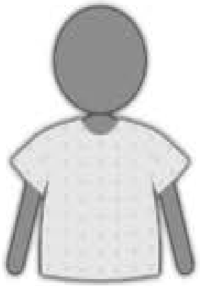
Health Care Providers

- Understand Rules
- Protect and Secure Information
- Educate Staff and Patients



Government

- Promotes Trust
- Develops Policies
- Fairly Enforces Rules



Patients

- Understand Rights
- Protect Personal Information
- Be Engaged

Technology Vendors

- Embrace Privacy by Design
- Provide Convenient Technology
- Implement Standards

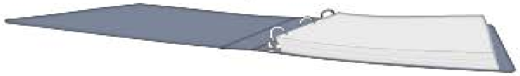
ONC Goal:
Inspire Confidence and Trust

Promote the Secure Use of Health IT

Information Assurance

Coordinate Development of Privacy and Security Policy

Patient Direct Access to Lab Report (CLIA)

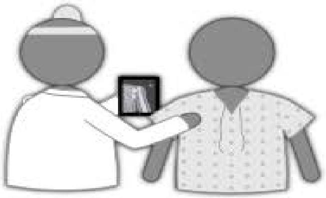


Meaningful Use

Educate and Empower Patients and Providers

Improved Access to Health Information

View and Download Health Records



Patient Education

Enhanced Understanding of Patients

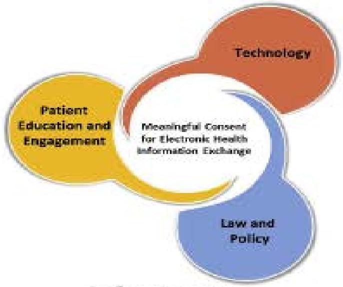
Provide Technical Assistance

Interactive Security Training

S&I FRAMEWORK

Data Segmentation for Privacy

Notice of Privacy Practices


Technology
Patient Education and Engagement
Meaningful Consent for Electronic Health Information Exchange
Law and Policy

eConsent Trial

Mobile Devices: Tips to Protect and Secure Health Information

Use a password or other user authentication.

Install and enable encryption.

Install and activate wiping and/or remote disabling.

Disable and do not install file-sharing applications.

Install and enable a firewall.

Install and enable security software.

Keep security software up to date.

Research mobile applications (apps) before downloading.

Maintain physical control of your mobile device.

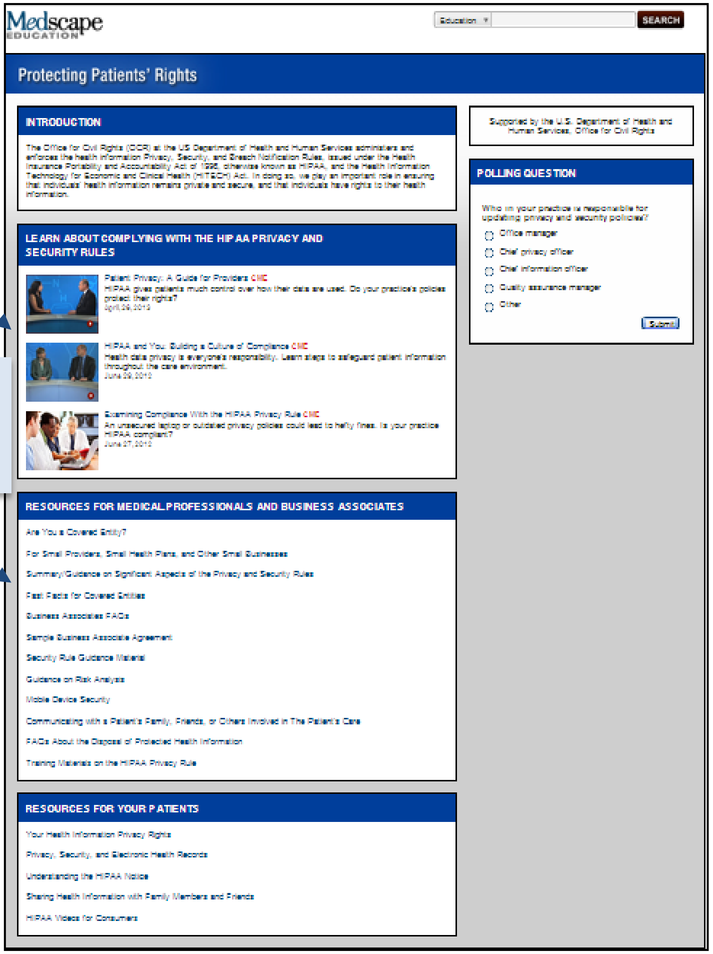
Use adequate security to send or receive health information over public Wi-Fi networks.

Delete all stored health information before discarding or reusing the mobile device.

Protecting Patients Rights:
New OCR Resource Center at Medscape.org

Video Programs module imbedded into page for dynamic interest

OCR Educational Links, Including Mobile Device Content



Protecting Patients' Rights

INTRODUCTION

The Office for Civil Rights (OCR) at the US Department of Health and Human Services administers and enforces the health information Privacy, Security, and Breach Notification Rules, issued under the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, and the Health Information Technology for Economic and Clinical Health (HITECH) Act. In doing so, we play an important role in ensuring that individuals' health information remains private and secure, and that individuals have rights to their health information.

LEARN ABOUT COMPLYING WITH THE HIPAA PRIVACY AND SECURITY RULES

Patient Privacy: A Guide for Providers CME
HIPAA gives patients much control over how their data are used. Do your practice's policies protect their rights?
April 26, 2012

HIPAA and You: Building a Culture of Compliance CME
Health data privacy is everyone's responsibility. Learn steps to safeguard patient information throughout the care environment.
June 29, 2012

Examining Compliance With the HIPAA Privacy Rule CME
An unsecured laptop or outdated privacy policies could lead to hefty fines. Is your practice HIPAA compliant?
June 27, 2012

RESOURCES FOR MEDICAL PROFESSIONALS AND BUSINESS ASSOCIATES

Are You a Covered Entity?

For Small Providers, Small Health Plans, and Other Small Businesses

Summary/Guidance on Significant Aspects of the Privacy and Security Rules

Fast Facts for Covered Entities

Business Associates FAQs

Sample Business Associate Agreement

Security Rule Guidance Material

Guidance on Risk Analysis

Mobile Device Security

Communicating with a Patient's Family, Friends, or Others Involved in The Patient's Care

FAQs About the Disposal of Protected Health Information

Training Materials on the HIPAA Privacy Rule

RESOURCES FOR YOUR PATIENTS

Your Health Information Privacy Rights

Privacy, Security, and Electronic Health Records

Understanding the HIPAA Notice

Sharing Health Information with Family Members and Friends

HIPAA Videos for Consumers

Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

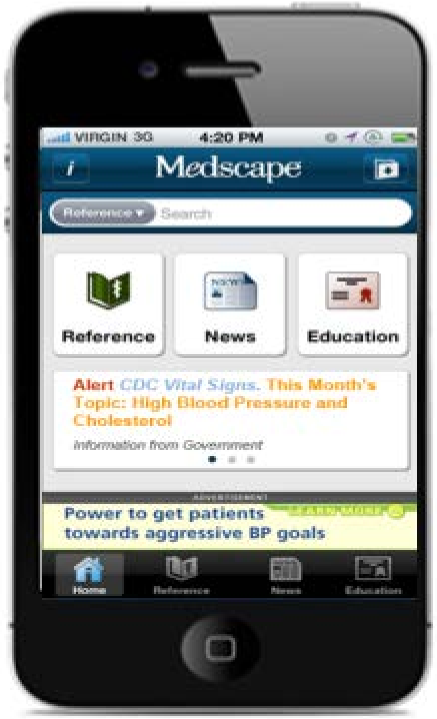
POLLING QUESTION

Who in your practice is responsible for updating privacy and security policies?

○ Office manager
○ Chief privacy officer
○ Chief information officer
○ Quality assurance manager
○ Other

Submit

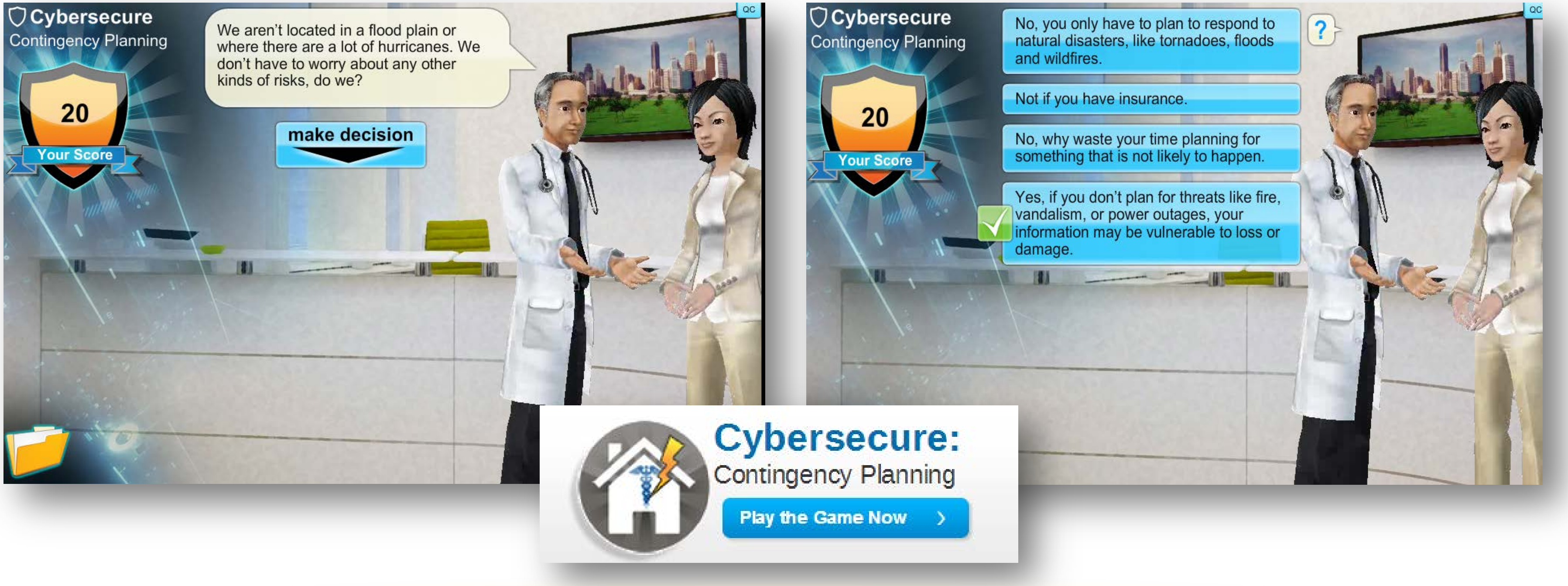
HIPAA/OCR Poll Question Updated Quarterly


VIRGIN 3G
4:20 PM
Medscape
Reference ▾
Search
Reference
News
Education
Alert CDC Vital Signs. This Month's Topic: High Blood Pressure and Cholesterol
Information from Government
ADVERTISEMENT
Power to get patients towards aggressive BP goals
LEARN MORE
Home
Reference
News
Education

http://www.medscape.org/sites/advances/patients-rights

Cybersecure: Contingency Planning

The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.



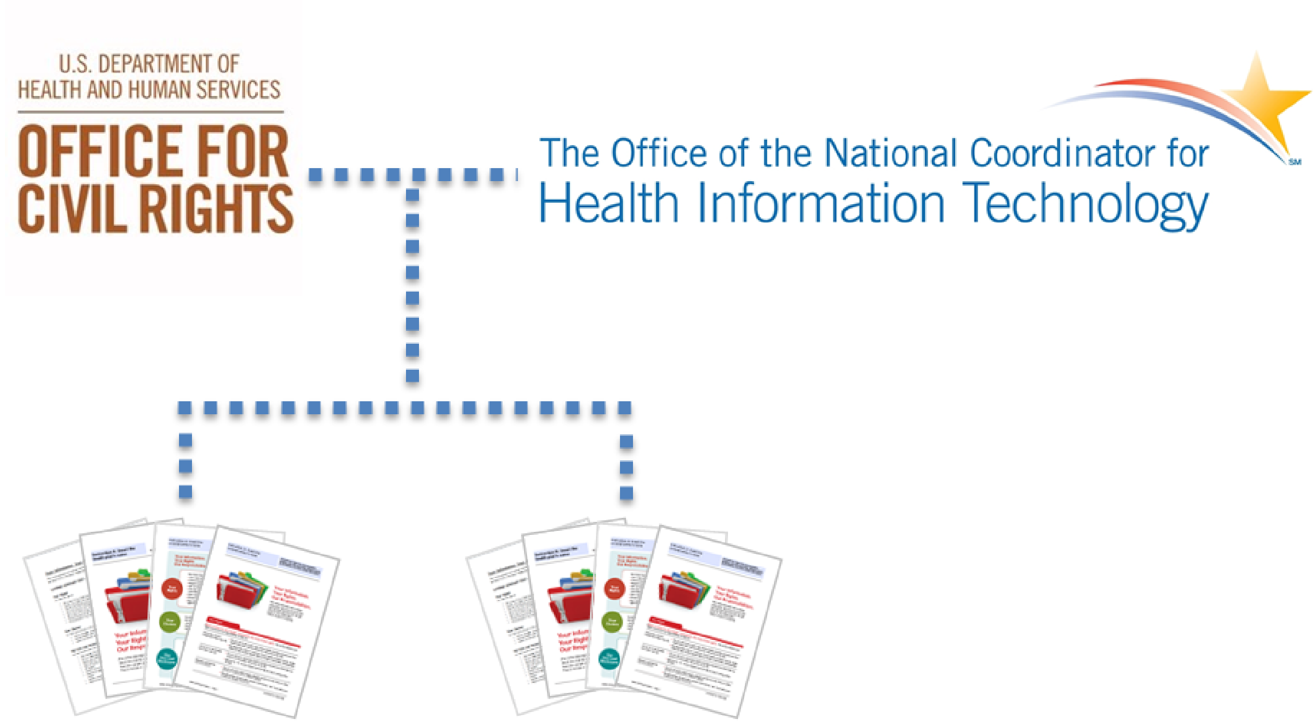
We aren't located in a flood plain or where there are a lot of hurricanes. We don't have to worry about any other kinds of risks, do we?

- No, you only have to plan to respond to natural disasters, like tornadoes, floods and wildfires.
- Not if you have insurance.
- No, why waste your time planning for something that is not likely to happen.
- ✓ Yes, if you don't plan for threats like fire, vandalism, or power outages, your information may be vulnerable to loss or damage.

http://www.healthit.gov/providers-professionals/privacy-security-training-games

Models of Notice of Privacy Practices

The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:



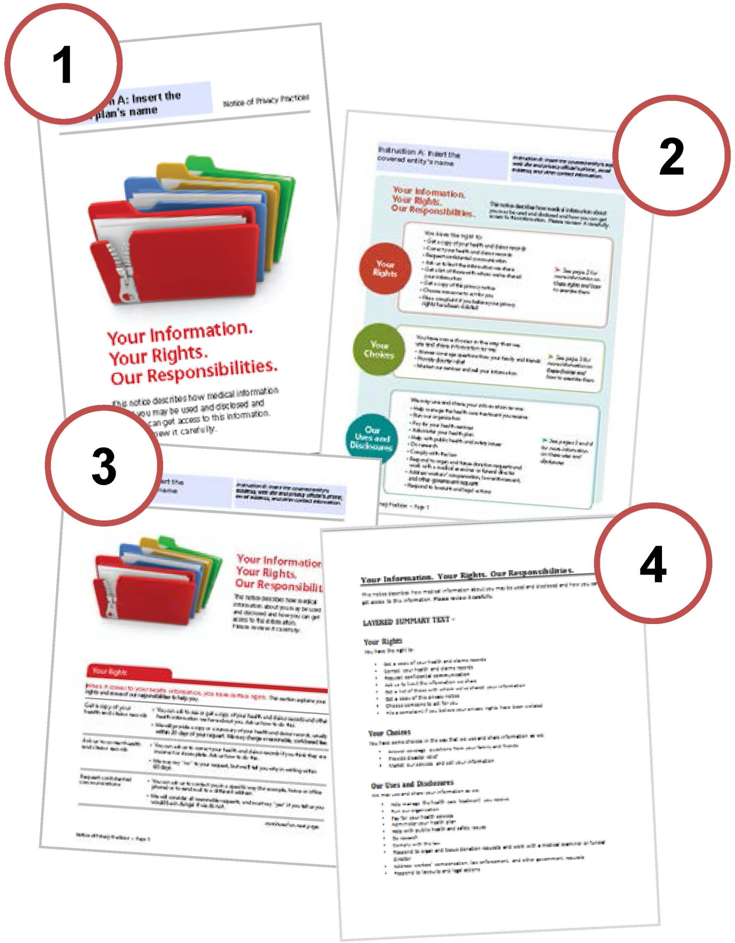
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

The Office of the National Coordinator for Health Information Technology

- ✓ One set for health plans
- ✓ One set for health care providers

Types of Notices Available

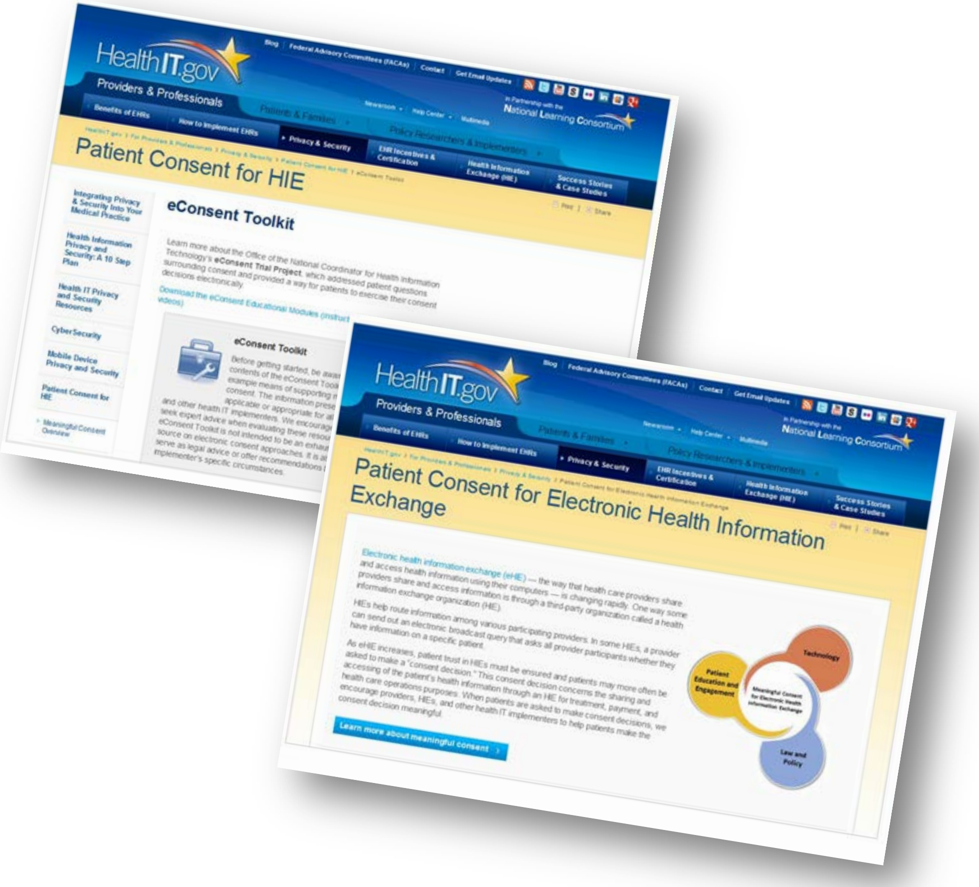


1. **Booklet** – Presents the material in booklet form with design elements
2. **Layered Notice** – Presents a summary of the information on the first page, followed by the full content on the following pages
3. **Full Page** – Has the design elements found in the booklet, but is formatted for full page presentation
4. **Text Only** – Provides a text-only version of the notice

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

Meaningful Consent Website

- Geared toward providers, health information exchange organizations (HIEs), and other health IT implementers
- Gives background on meaningful consent and ONC’s eConsent Trial Project
- Provides customizable tools and resources to help you enable patients to make meaningful consent decisions


HealthIT.gov
Providers & Professionals
Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates
Newsroom | Help Center | Multimedia
In Partnership with the National Learning Consortium
Patients & Families
Policy Researchers & Implementers
Benefits of EHRs
How to Implement EHRs
Privacy & Security
EHR Incentives & Certification
Health Information Exchange (HIE)
Success Stories & Case Studies
HealthIT.gov › For Providers & Professionals › Privacy & Security › Patient Consent for HIE › eConsent Toolkit
Print | Share
Integrating Privacy & Security Into Your Medical Practice
Health Information Privacy and Security: A 10 Step Plan
Health IT Privacy and Security Resources
CyberSecurity
Mobile Device Privacy and Security
Patient Consent for HIE
Meaningful Consent Overview
HealthIT.gov › For Providers & Professionals › Privacy & Security › Patient Consent for Electronic Health Information Exchange
Technology
Patient Education and Engagement
Meaningful Consent for Electronic Health Information Exchange
Law and Policy

Patient Consent for HIE

eConsent Toolkit

Learn more about the Office of the National Coordinator for Health Information Technology's **eConsent Trial Project**, which addressed patient questions surrounding consent and provided a way for patients to exercise their consent decisions electronically.

Download the eConsent Educational Modules (instruct videos)

eConsent Toolkit

Before getting started, be awa contents of the eConsent Tool example means of supporting consent. The information prese applicable or appropriate for a and other health IT implementers. We encourag seek expert advice when evaluating these resou eConsent Toolkit is not intended to be an exhau source on electronic consent approaches. It is a serve as legal advice or offer recommendations implementer's specific circumstances.

Patient Consent for Electronic Health Information Exchange

Electronic health information exchange (eHIE) — the way that health care providers share and access health information using their computers — is changing rapidly. One way some providers share and access information is through a third-party organization called a health information exchange organization (HIE).

HIEs help route information among various participating providers. In some HIEs, a provider can send out an electronic broadcast query that asks all provider participants whether they have information on a specific patient.

As eHIE increases, patient trust in HIEs must be ensured and patients may more often be asked to make a "consent decision." This consent decision concerns the sharing and accessing of the patient's health information through an HIE for treatment, payment, and health care operations purposes. When patients are asked to make consent decisions, we encourage providers, HIEs, and other health IT implementers to help patients make the consent decision meaningful.

Learn more about meaningful consent ›

www.HealthIT.gov/meaningfulconsent

Security 101: Contingency Planning

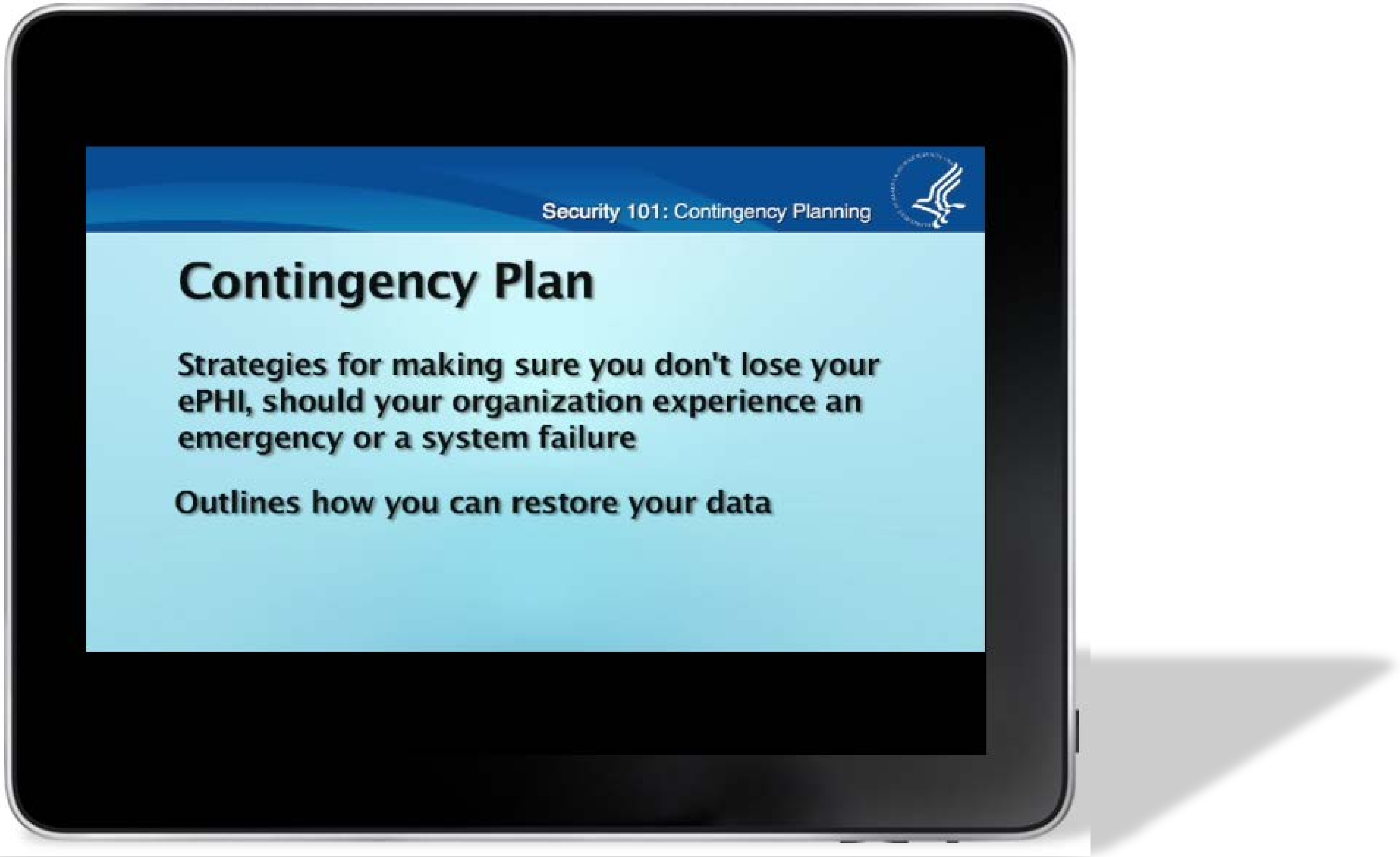
Security 101: Contingency Planning

Contingency Plan

www.HealthIT.gov/security-risk-assessment

Security 101: Contingency Planning

A contingency plan is a way to establish strategies for making sure you don't lose your ePHI, should your organization experience an emergency or a system failure. A contingency plan also o utlines how you can restore your data. If you do suffer a data loss.



Security 101: Contingency Planning

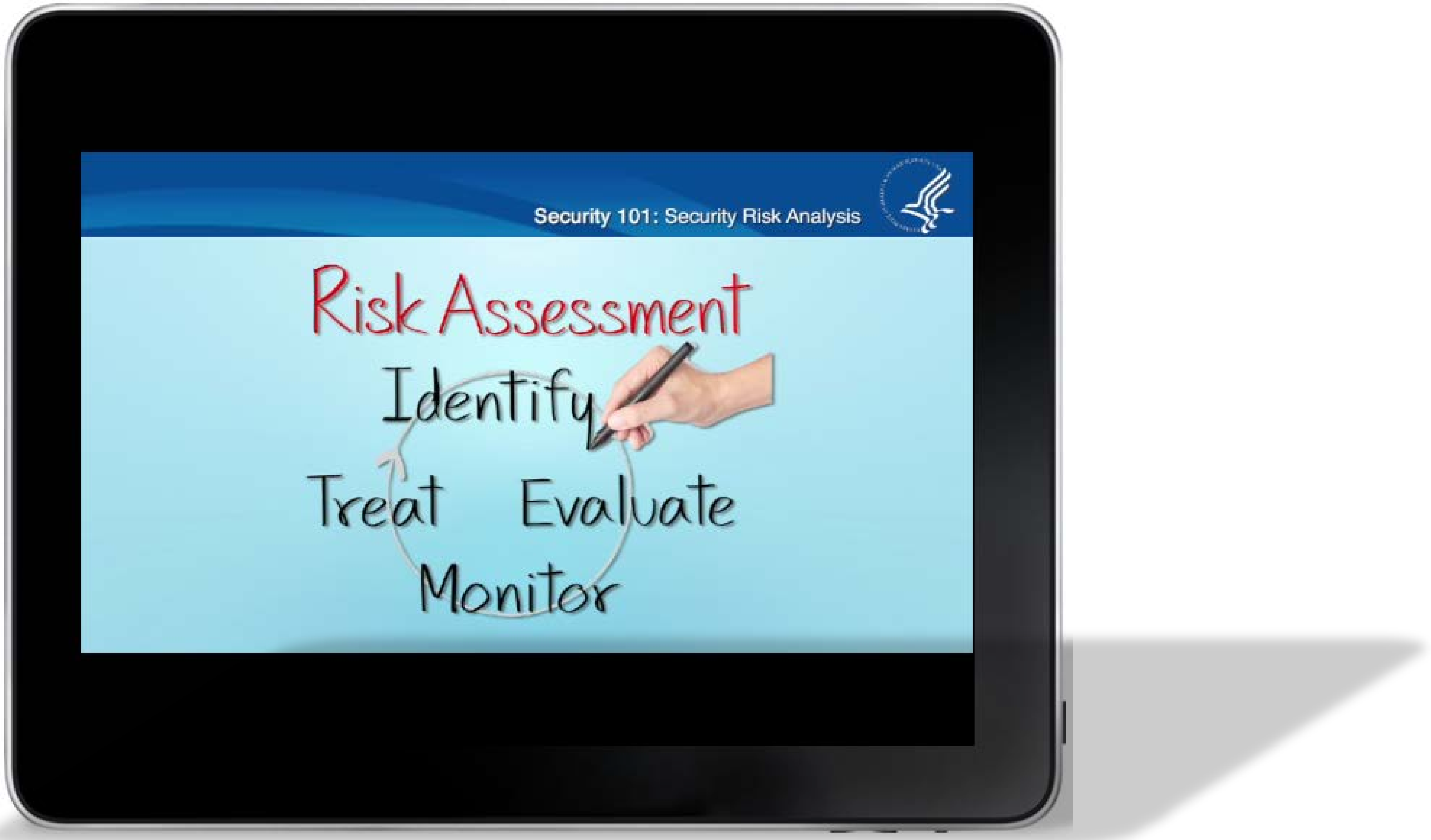
Contingency Plan

Strategies for making sure you don't lose your ePHI, should your organization experience an emergency or a system failure

Outlines how you can restore your data

Security 101: Security Risk Analysis

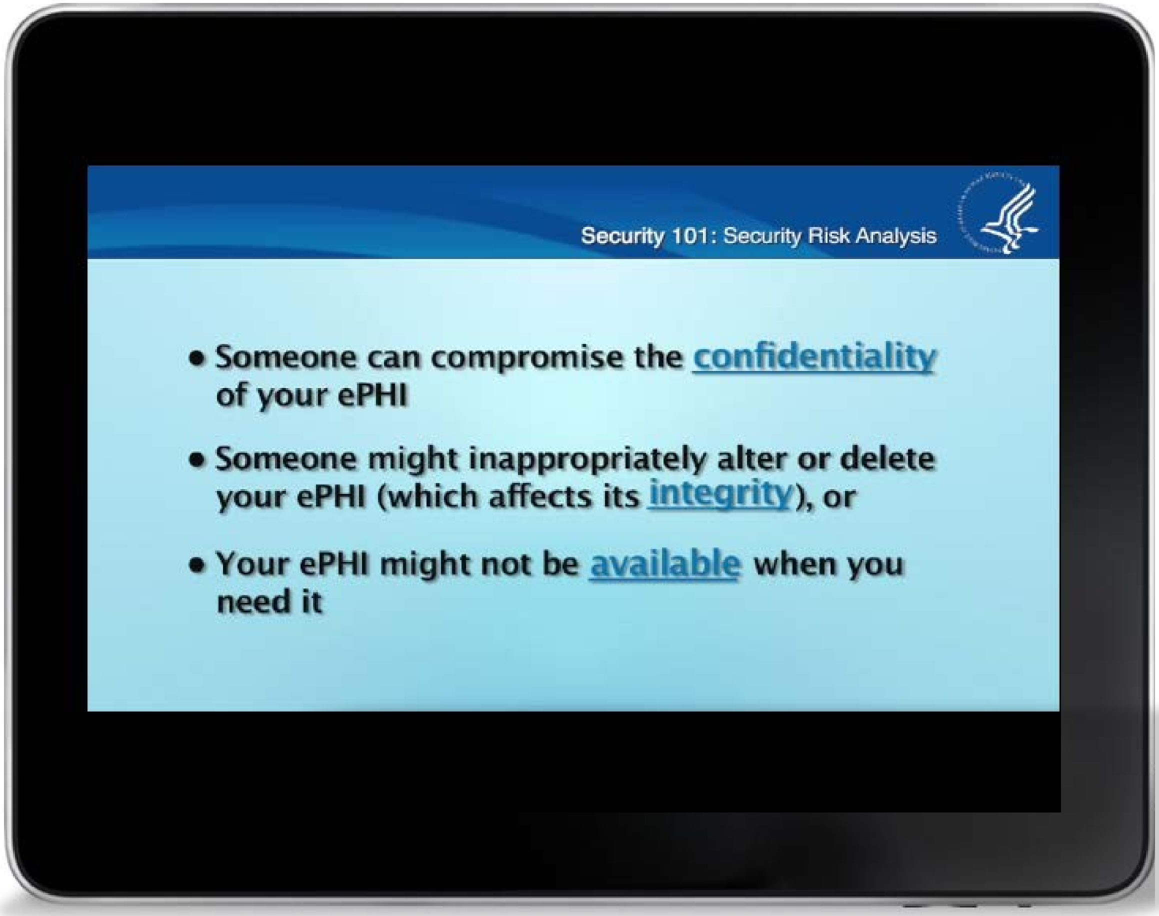
A Risk Analysis is seen as one of the most important security tasks. Performing a Risk Analysis will help you identify when and where there is a risk…



www.HealthIT.gov/security-risk-assessment

Security 101: Security Risk Analysis

A risk where…

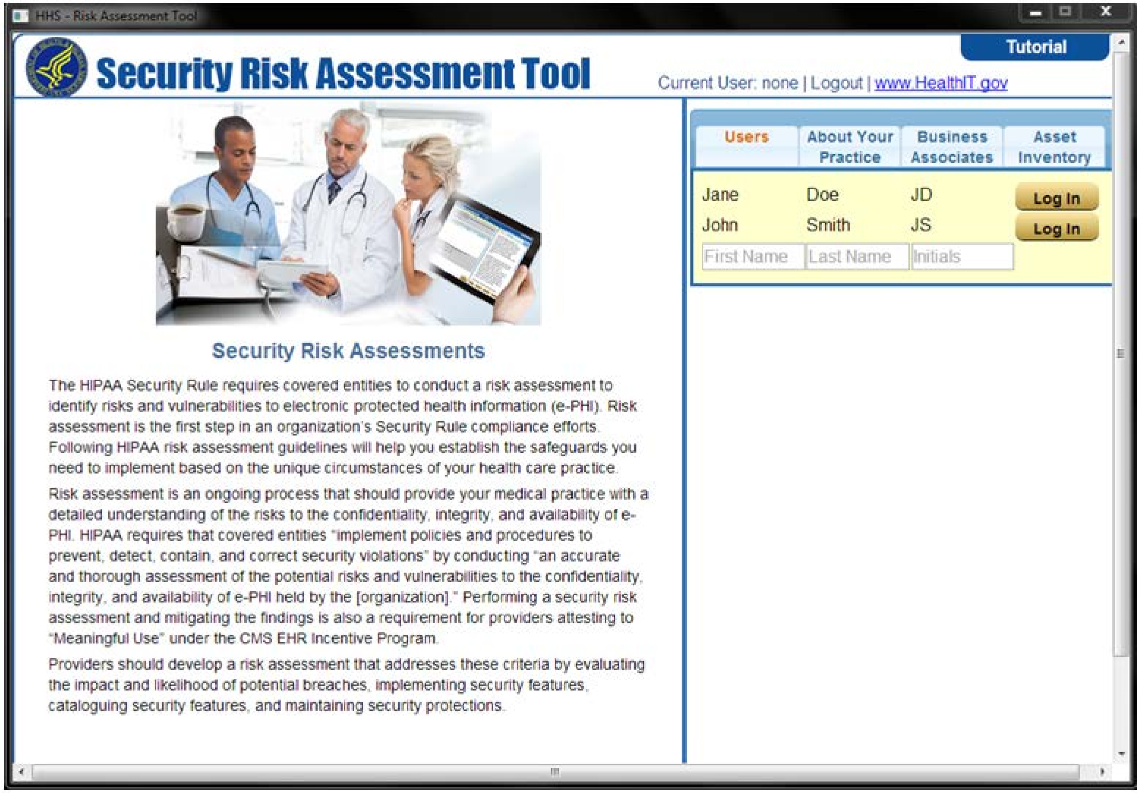


Security 101: Security Risk Analysis

- Someone can compromise the confidentiality of your ePHI
- Someone might inappropriately alter or delete your ePHI (which affects its integrity), or
- Your ePHI might not be available when you need it

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool



Security Risk Assessment Tool

Current User: none | Logout | www.HealthIT.gov

Jane	Doe	JD	Log In
John	Smith	JS	Log In
First Name	Last Name	Initials	

Security Risk Assessments

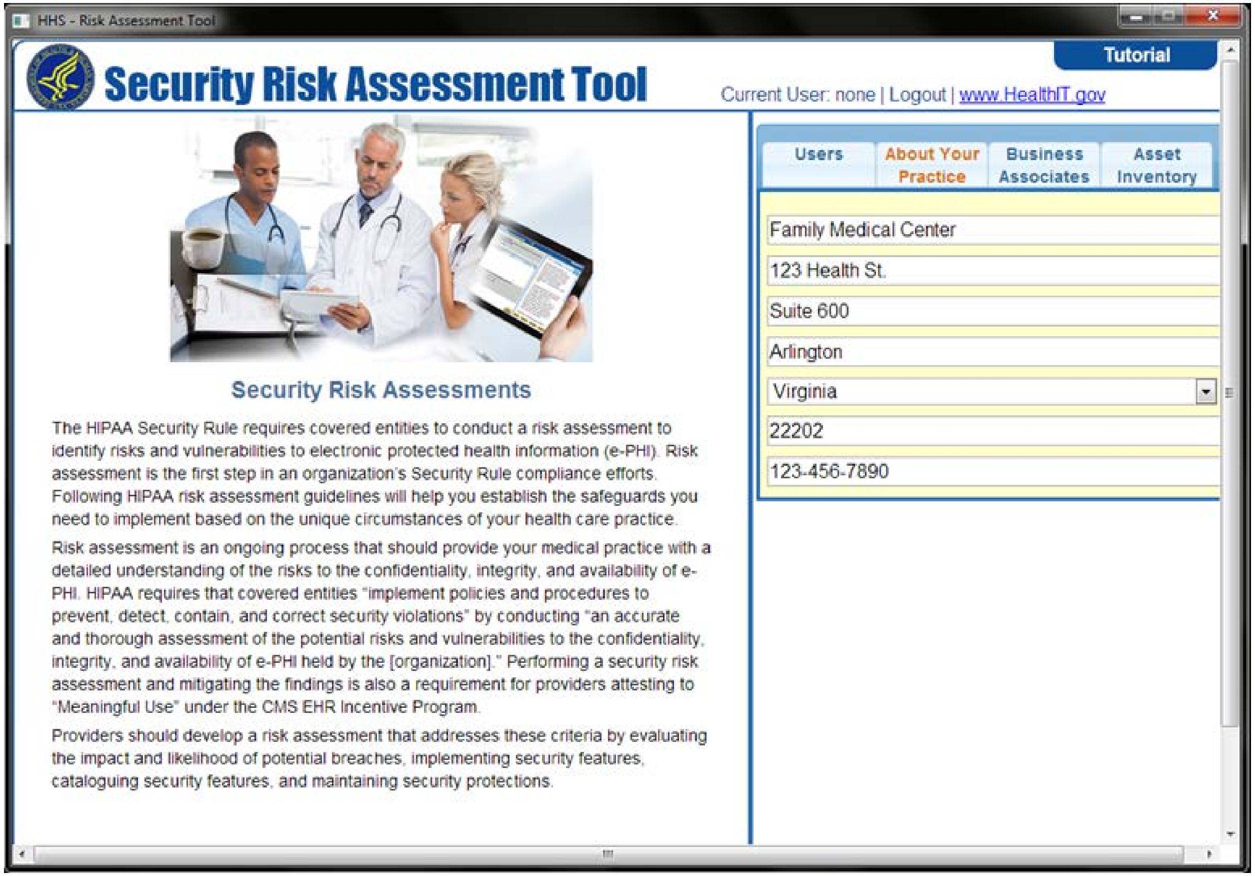
The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: none | Logout | www.HealthIT.gov
Users
About Your Practice
Business Associates
Asset Inventory

Family Medical Center

123 Health St.

Suite 600

Arlington

Virginia

22202

123-456-7890

Security Risk Assessments

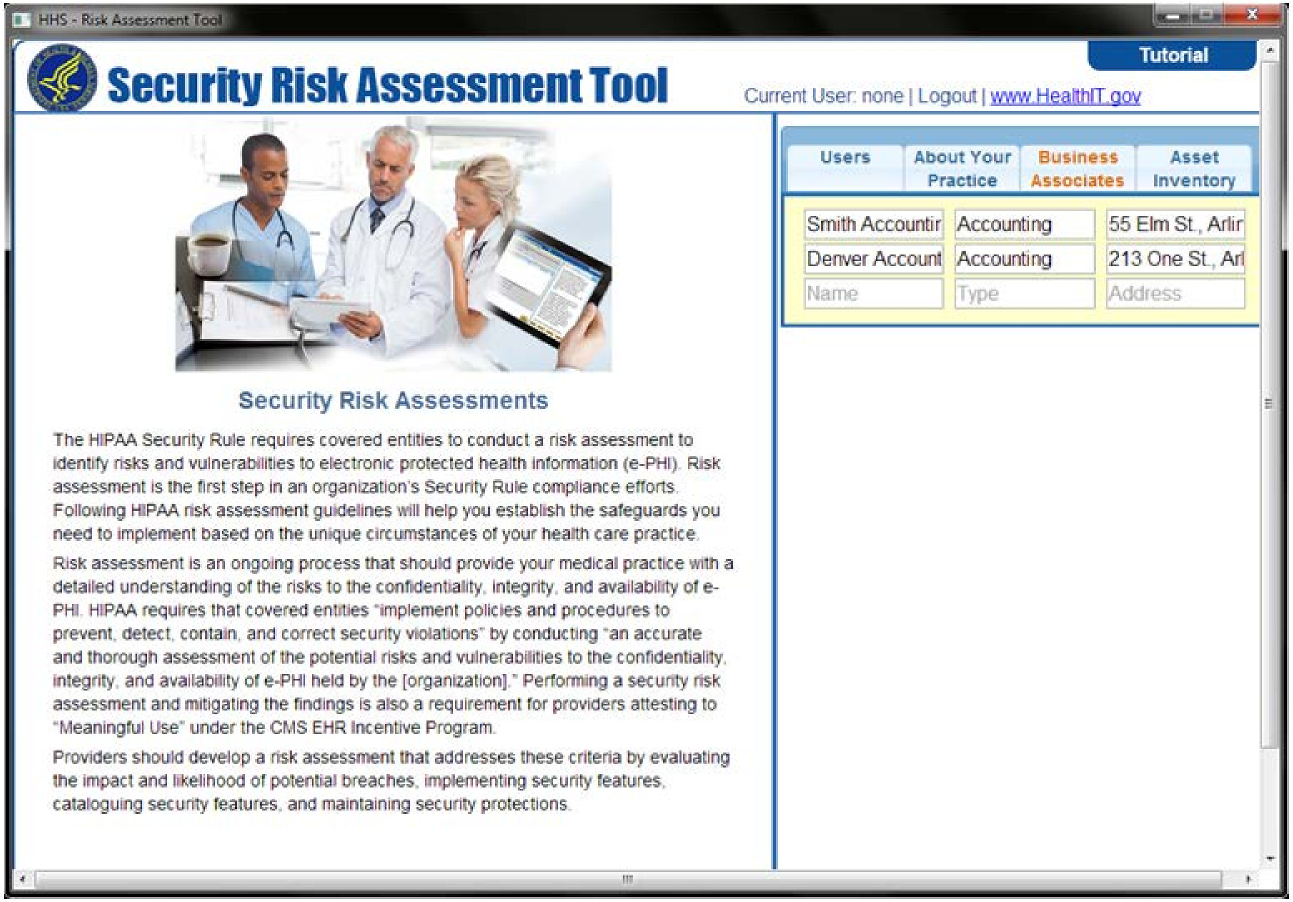
The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: none | Logout | www.HealthIT.gov
Users
About Your Practice
Business Associates
Asset Inventory

Smith Accountir	Accounting	55 Elm St., Arlir
Denver Account	Accounting	213 One St., Arl
Name	Type	Address

Security Risk Assessments

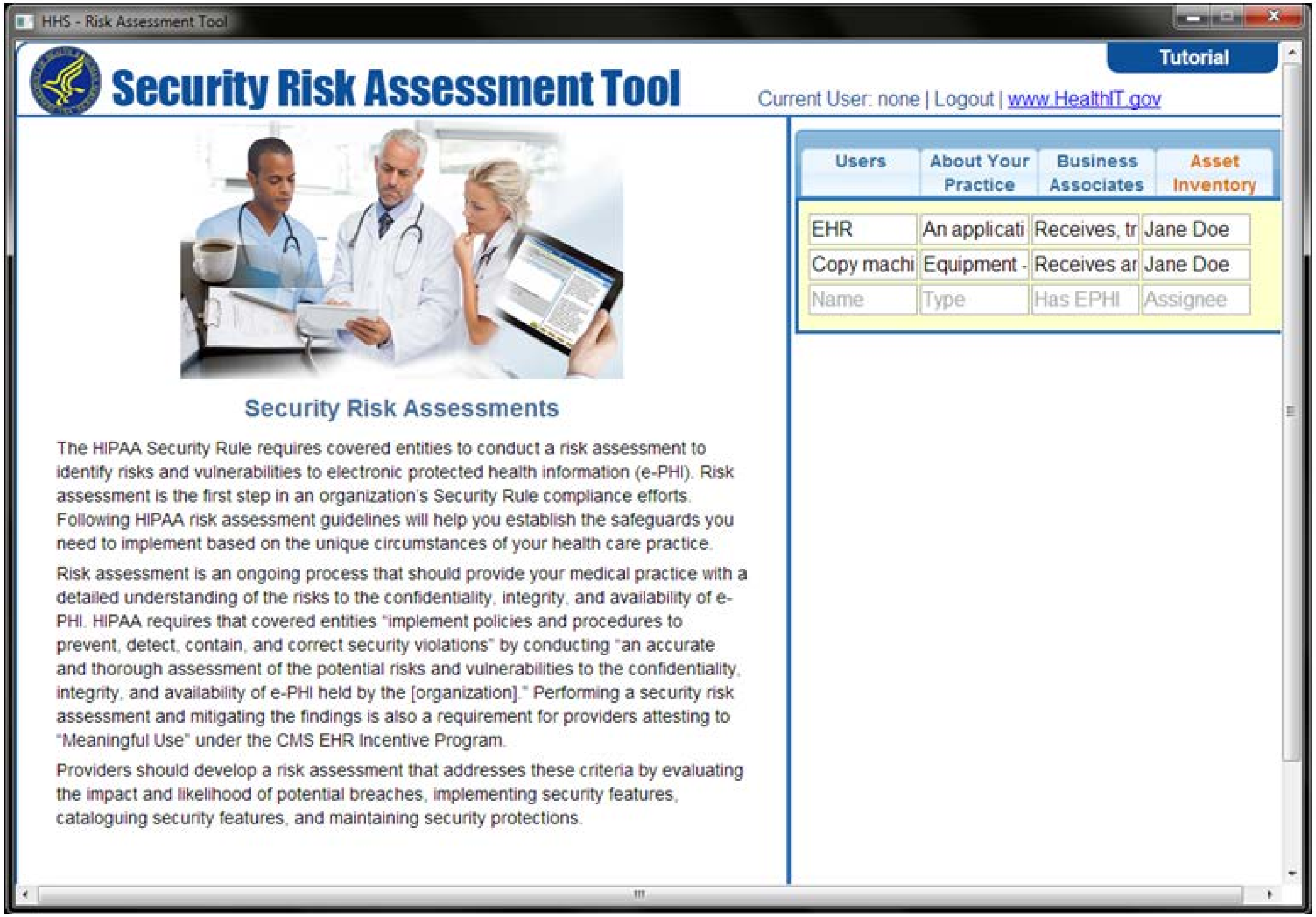
The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

www.HealthIT.gov/security-risk-assessment

Coming Soon: Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: none | Logout | www.HealthIT.gov
Users
About Your Practice
Business Associates
Asset Inventory

EHR	An applicati	Receives, tr	Jane Doe
Copy machi	Equipment -	Receives ar	Jane Doe
Name	Type	Has EPHI	Assignee

Security Risk Assessments

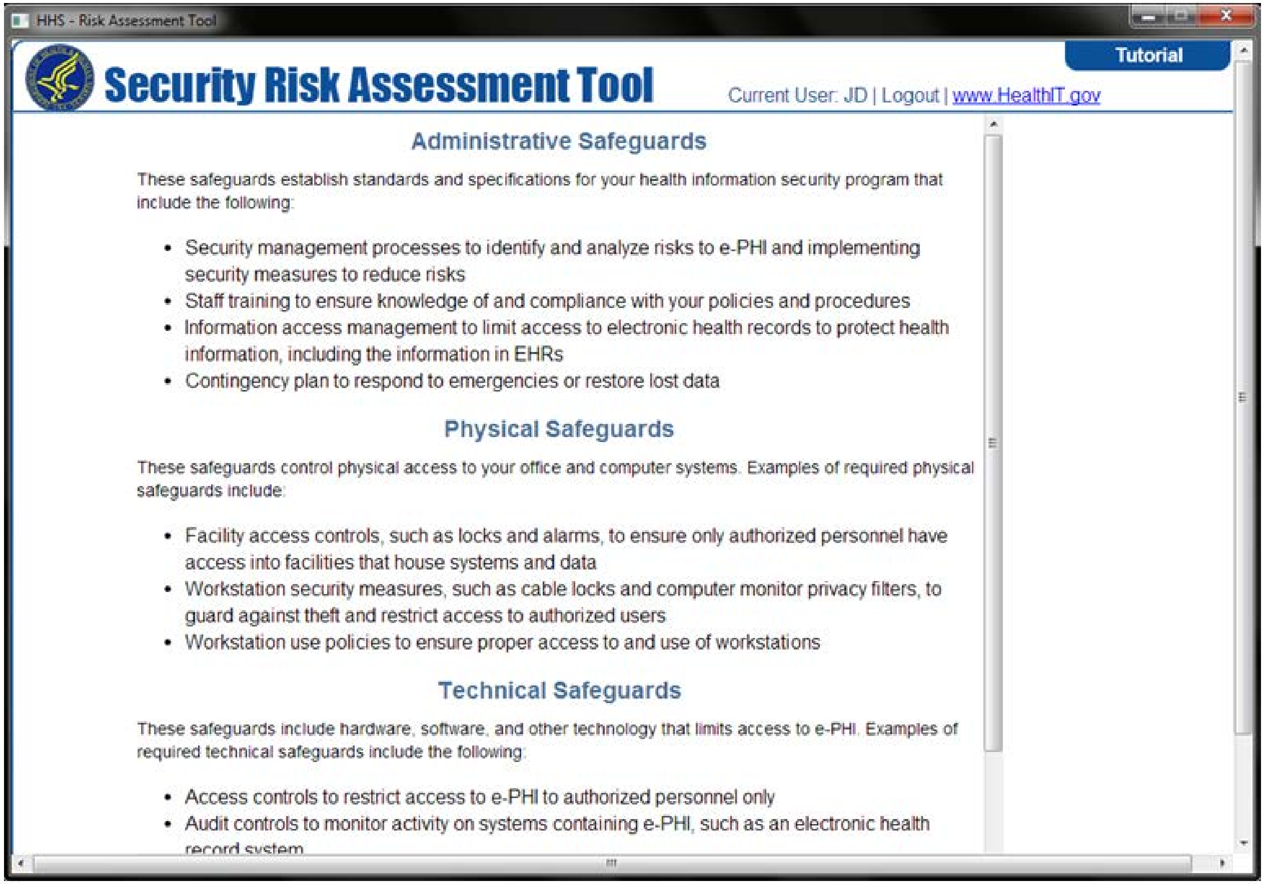
The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Tutorial
Security Risk Assessment Tool
Current User: JD | Logout | www.HealthIT.gov

Administrative Safeguards

These safeguards establish standards and specifications for your health information security program that include the following:

- Security management processes to identify and analyze risks to e-PHI and implementing security measures to reduce risks
- Staff training to ensure knowledge of and compliance with your policies and procedures
- Information access management to limit access to electronic health records to protect health information, including the information in EHRs
- Contingency plan to respond to emergencies or restore lost data

Physical Safeguards

These safeguards control physical access to your office and computer systems. Examples of required physical safeguards include:

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users
- Workstation use policies to ensure proper access to and use of workstations

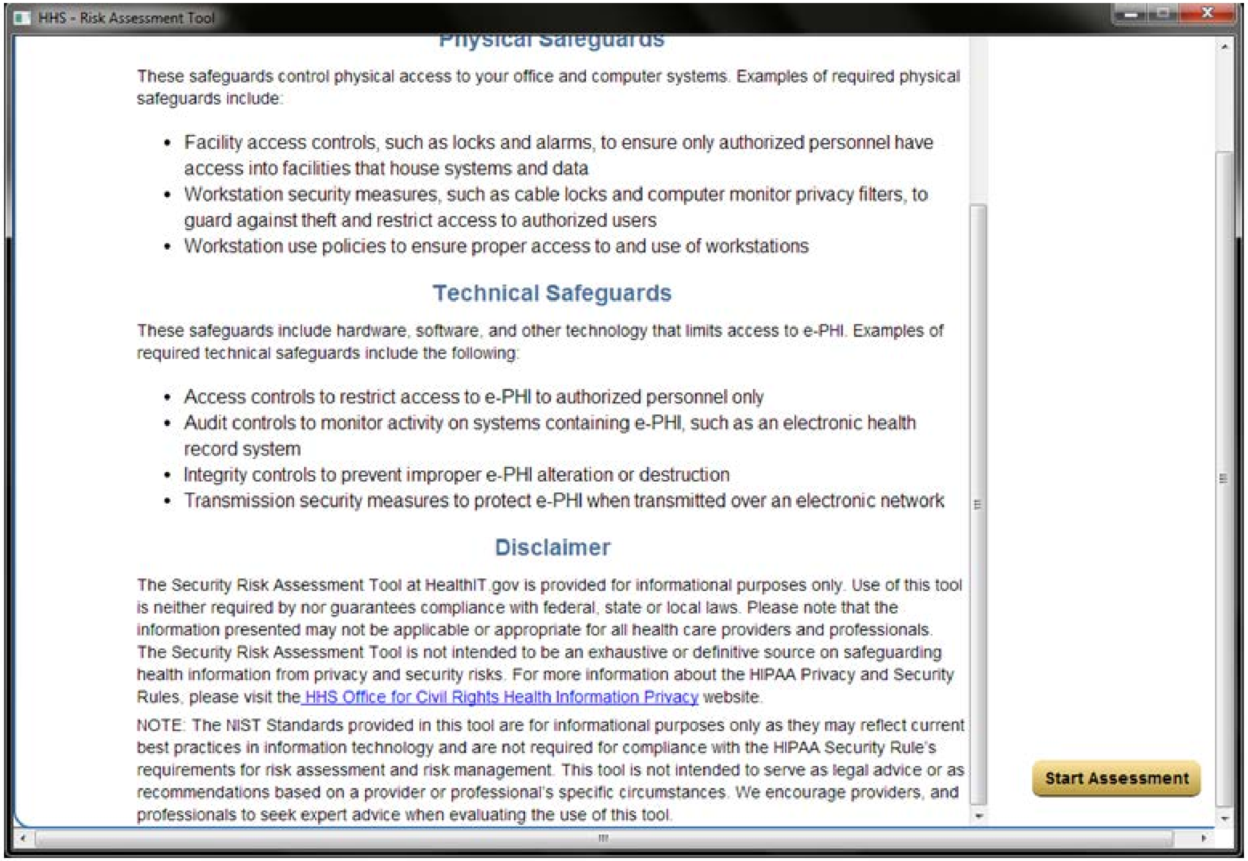
Technical Safeguards

These safeguards include hardware, software, and other technology that limits access to e-PHI. Examples of required technical safeguards include the following:

- Access controls to restrict access to e-PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool



Physical Safeguards

These safeguards control physical access to your office and computer systems. Examples of required physical safeguards include:

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users
- Workstation use policies to ensure proper access to and use of workstations

Technical Safeguards

These safeguards include hardware, software, and other technology that limits access to e-PHI. Examples of required technical safeguards include the following:

- Access controls to restrict access to e-PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper e-PHI alteration or destruction
- Transmission security measures to protect e-PHI when transmitted over an electronic network

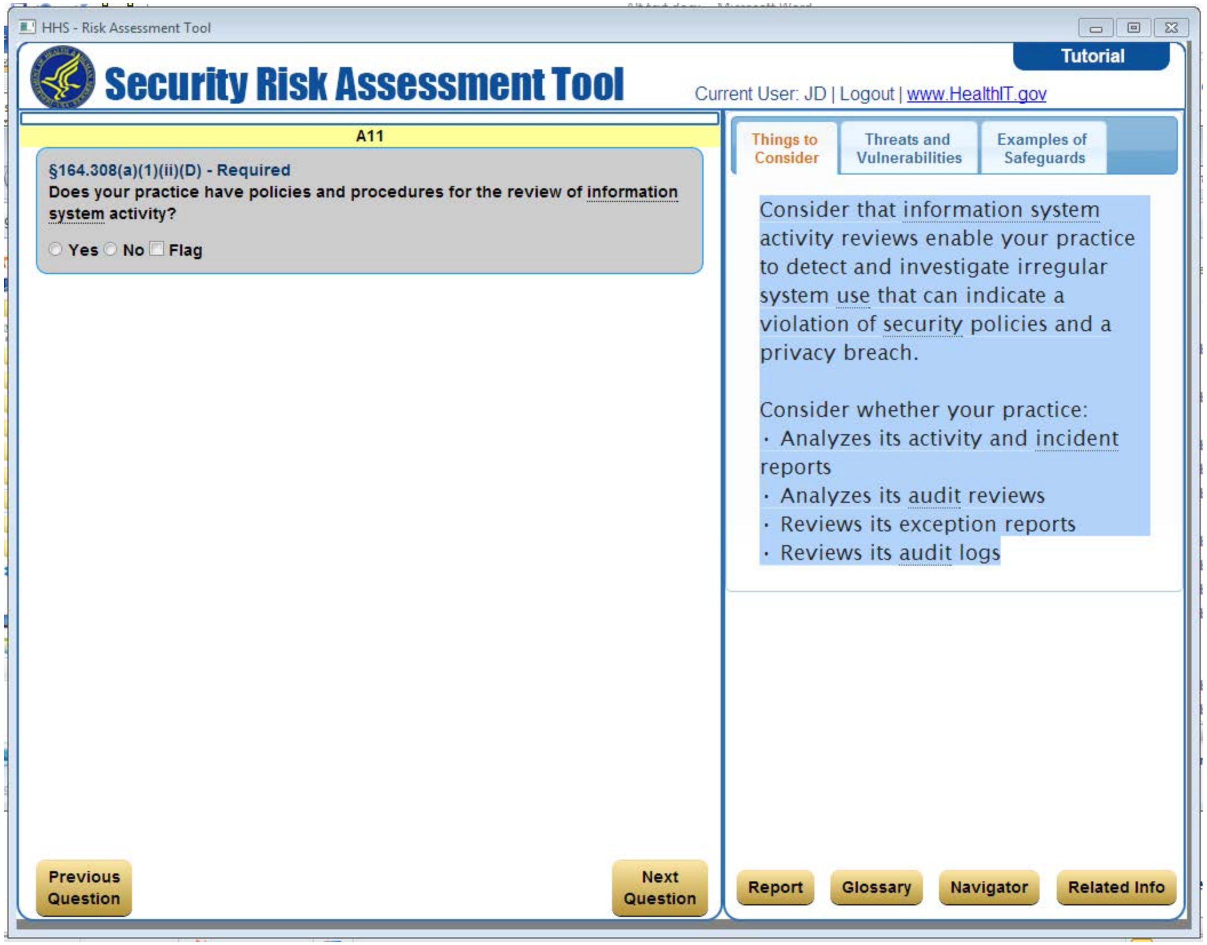
Disclaimer

The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website.

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: JD | Logout | www.HealthIT.gov
A11
Things to Consider
Threats and Vulnerabilities
Examples of Safeguards
Previous Question
Next Question
Report
Glossary
Navigator
Related Info

§164.308(a)(1)(ii)(D) - Required

Does your practice have policies and procedures for the review of information system activity?

○ Yes ○ No □ Flag

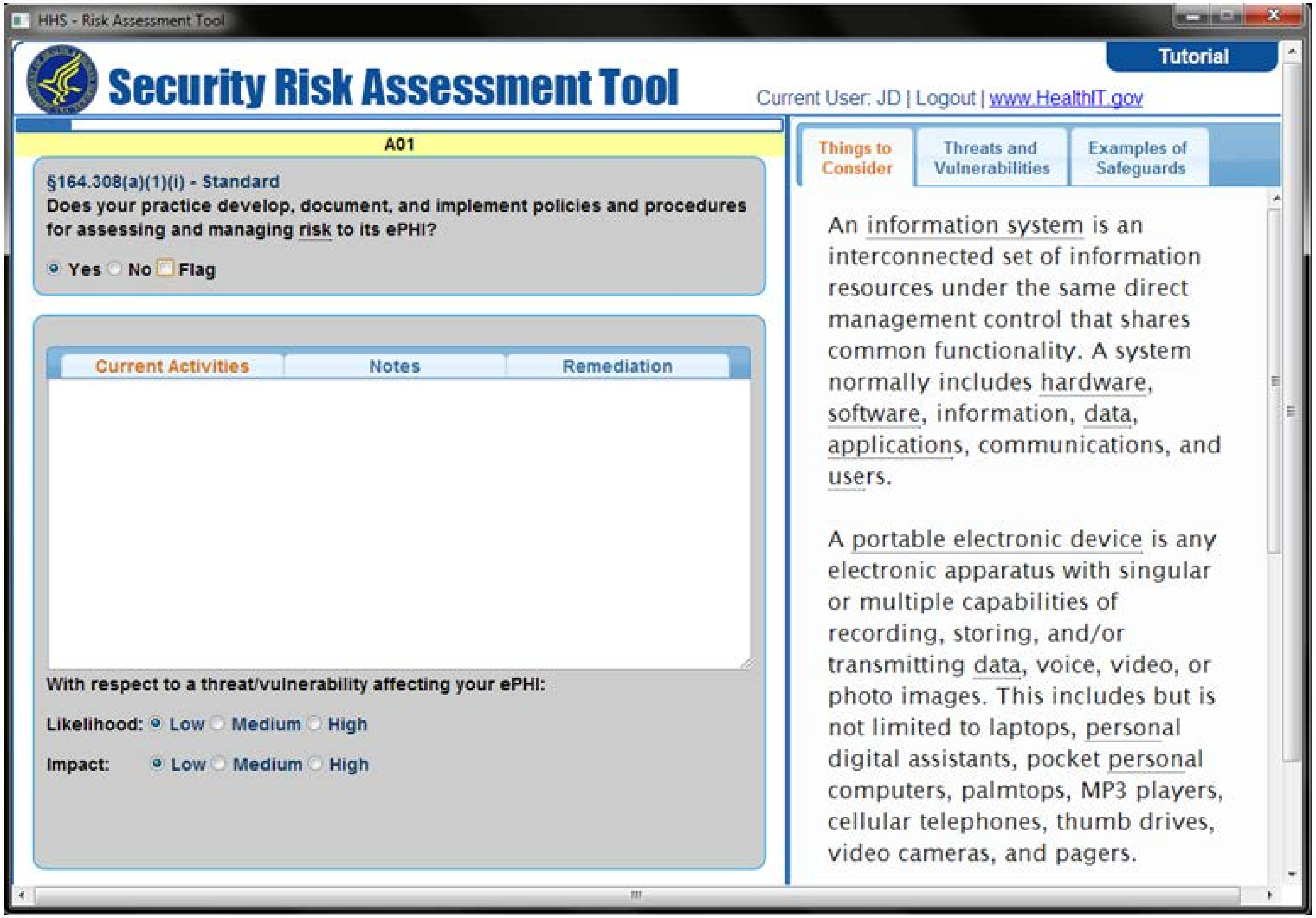
Consider that information system activity reviews enable your practice to detect and investigate irregular system use that can indicate a violation of security policies and a privacy breach.

Consider whether your practice:

- Analyzes its activity and incident reports
- Analyzes its audit reviews
- Reviews its exception reports
- Reviews its audit logs

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: JD | Logout | www.HealthIT.gov
A01
Things to Consider
Threats and Vulnerabilities
Examples of Safeguards
Current Activities
Notes
Remediation

§164.308(a)(1)(i) - Standard

Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

● Yes ○ No □ Flag

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ● Low ○ Medium ○ High

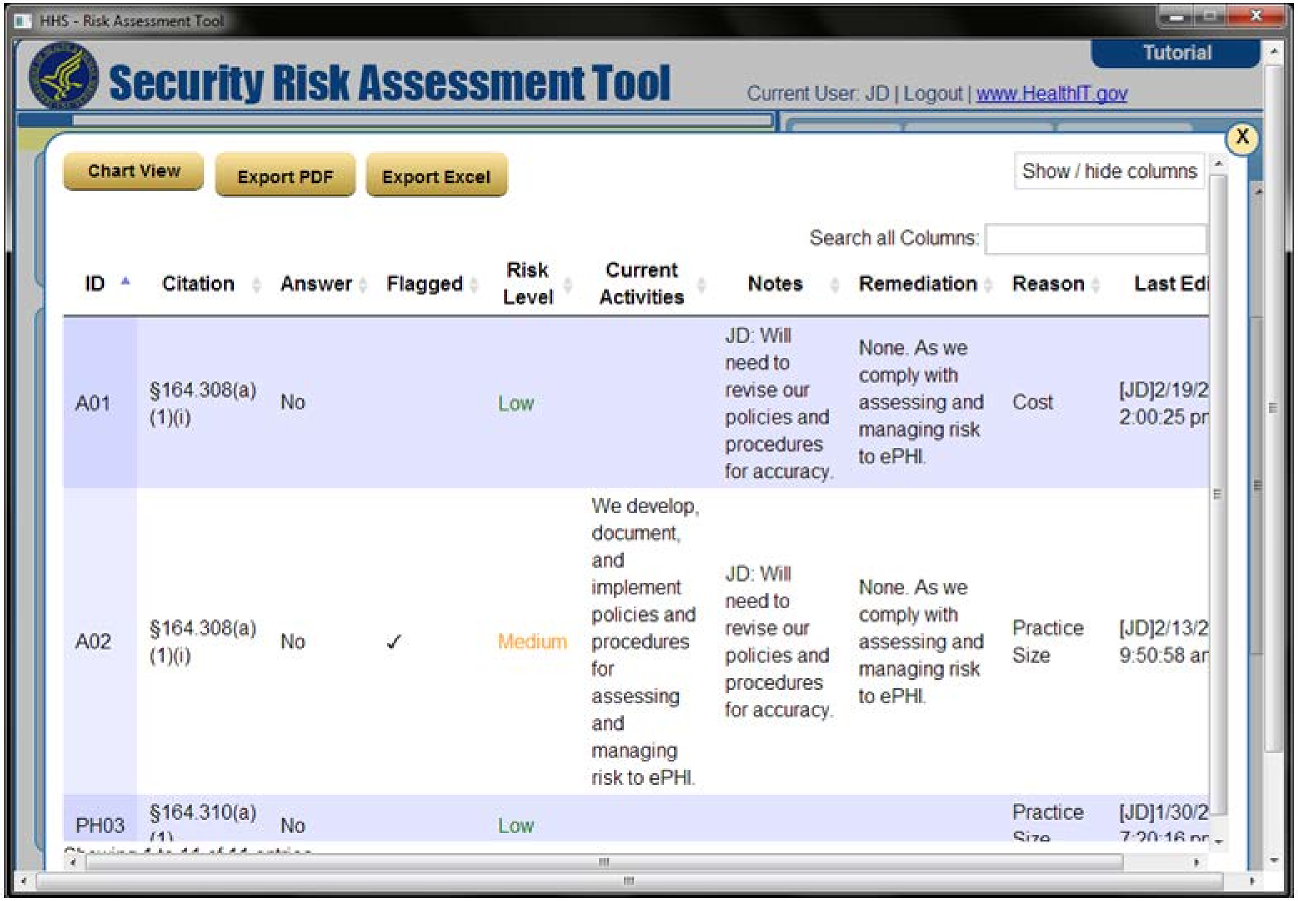
Impact: ● Low ○ Medium ○ High

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool



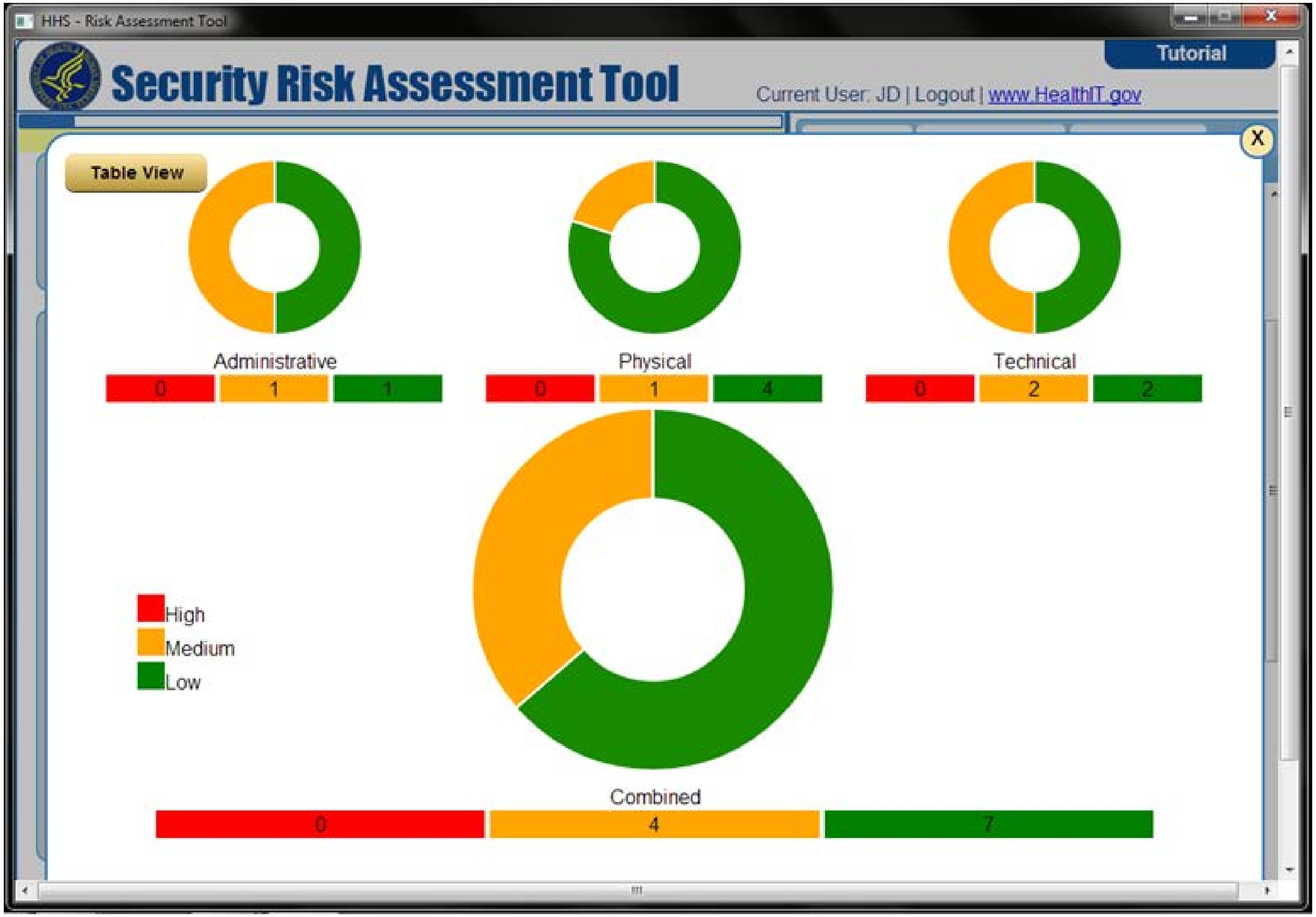
HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: JD | Logout | www.HealthIT.gov
Chart View
Export PDF
Export Excel
Show / hide columns
Search all Columns:

ID	Citation	Answer	Flagged	Risk Level	Current Activities	Notes	Remediation	Reason	Last Edi
A01	§164.308(a)(1)(i)	No		Low		JD: Will need to revise our policies and procedures for accuracy.	None. As we comply with assessing and managing risk to ePHI.	Cost	[JD]2/19/2 2:00:25 pr
A02	§164.308(a)(1)(i)	No	✓	Medium	We develop, document, and implement policies and procedures for assessing and managing risk to ePHI.	JD: Will need to revise our policies and procedures for accuracy.	None. As we comply with assessing and managing risk to ePHI.	Practice Size	[JD]2/13/2 9:50:58 ar
PH03	§164.310(a)(1)	No		Low				Practice Size	[JD]1/30/2 7:20:16 pr

Showing 1 to 11 of 11 entries

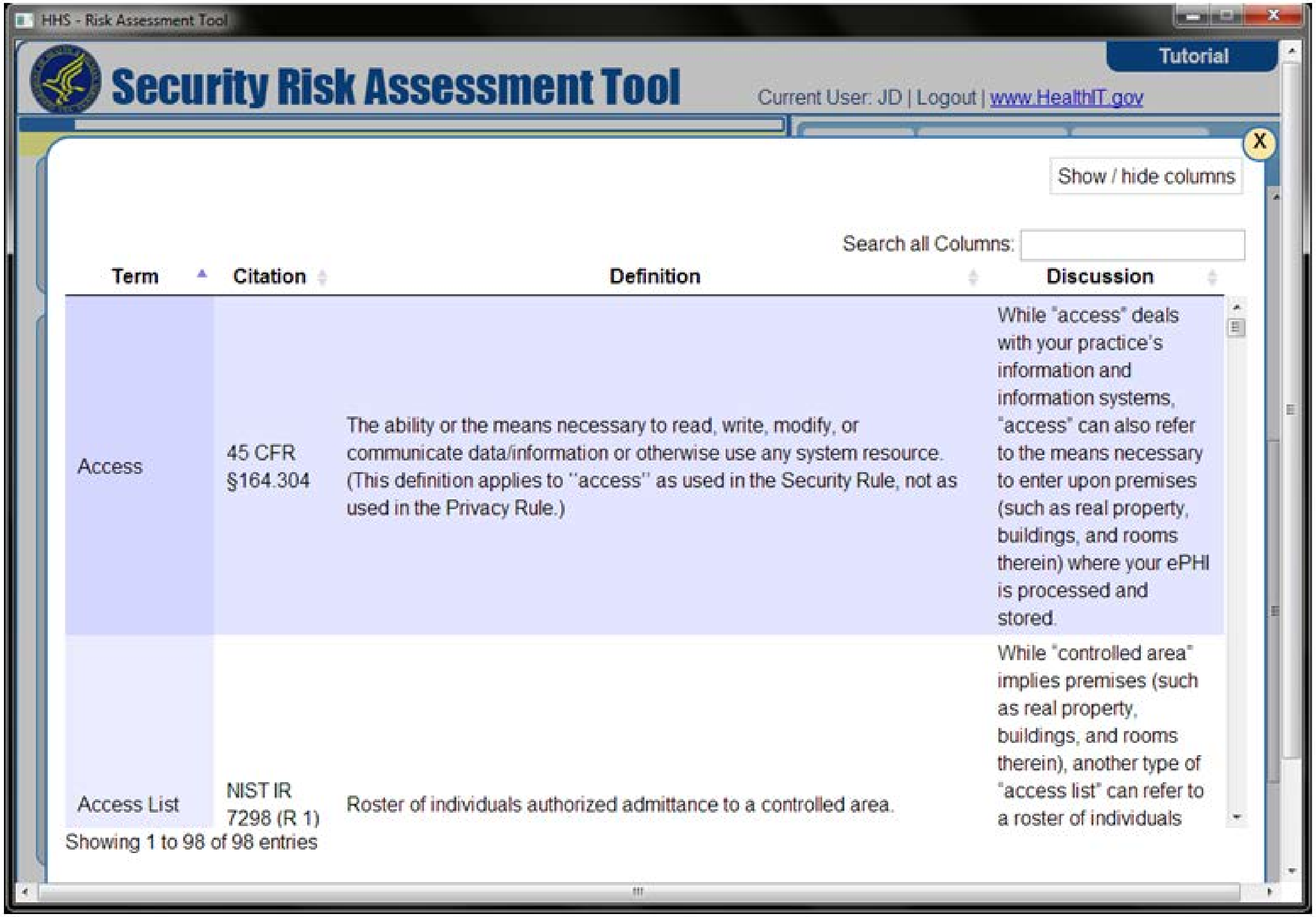
www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: JD | Logout | www.HealthIT.gov
Table View
X
Administrative
0
1
1
Physical
0
1
4
Technical
0
2
2
🟥 High
🟧 Medium
🟩 Low
Combined
0
4
7

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool



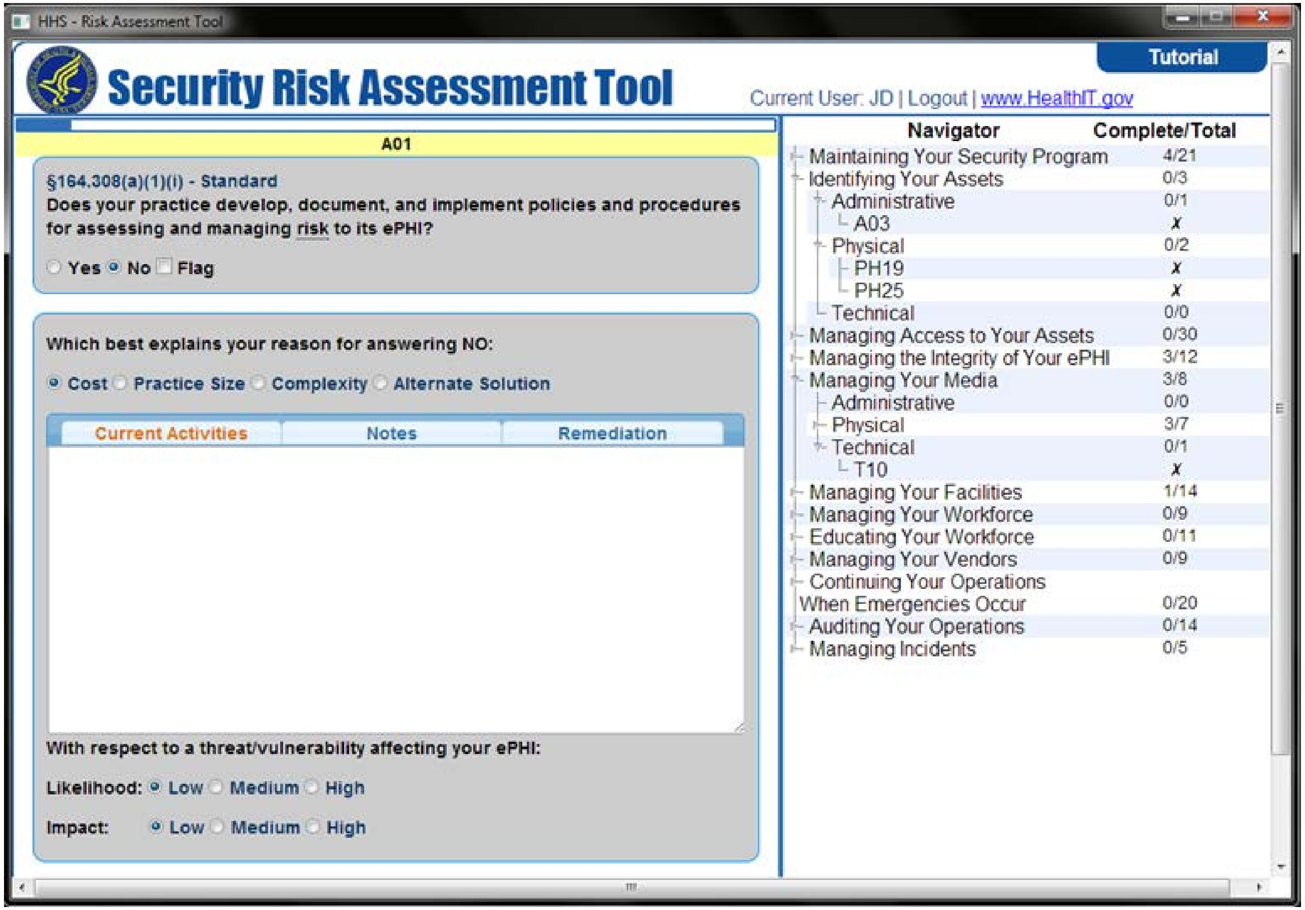
HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: JD | Logout | www.HealthIT.gov
X
Show / hide columns
Search all Columns:

Term	Citation	Definition	Discussion
Access	45 CFR §164.304	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in the Security Rule, not as used in the Privacy Rule.)	While "access" deals with your practice's information and information systems, "access" can also refer to the means necessary to enter upon premises (such as real property, buildings, and rooms therein) where your ePHI is processed and stored.
Access List	NIST IR 7298 (R 1)	Roster of individuals authorized admittance to a controlled area.	While "controlled area" implies premises (such as real property, buildings, and rooms therein), another type of "access list" can refer to a roster of individuals

Showing 1 to 98 of 98 entries

www.HealthIT.gov/security-risk-assessment

Coming Soon - Security Risk Assessment Tool



Security Risk Assessment Tool

Current User: JD | Logout | www.HealthIT.gov

A01

§164.308(a)(1)(i) - Standard

Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

○ Yes ● No □ Flag

Which best explains your reason for answering NO:

● Cost ○ Practice Size ○ Complexity ○ Alternate Solution

Current Activities | Notes | Remediation

With respect to a threat/vulnerability affecting your ePHI:

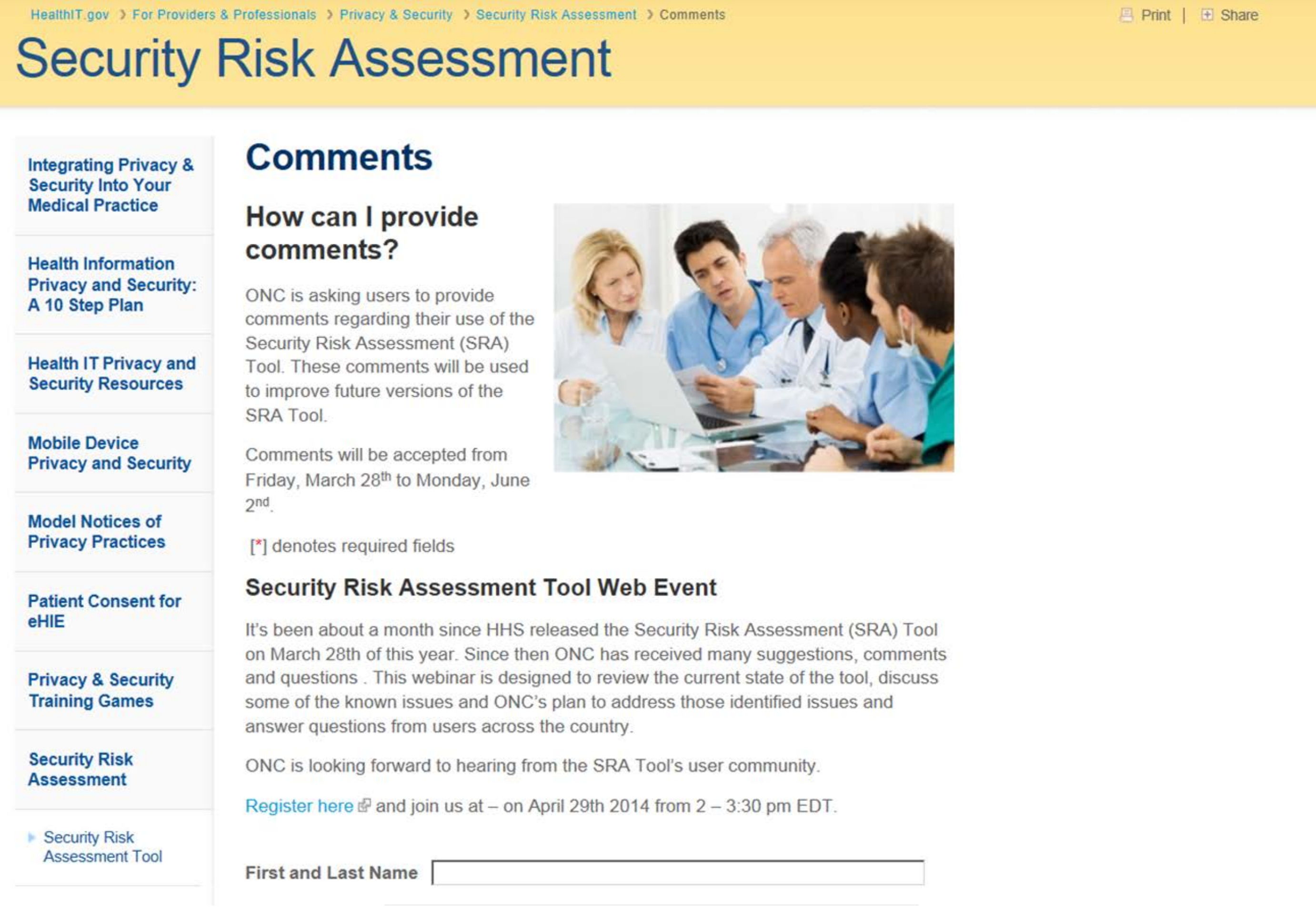
Likelihood: ● Low ○ Medium ○ High

Impact: ● Low ○ Medium ○ High

Navigator	Complete/Total
Maintaining Your Security Program	4/21
Identifying Your Assets	0/3
Administrative	0/1
A03	✗
Physical	0/2
PH19	✗
PH25	✗
Technical	0/0
Managing Access to Your Assets	0/30
Managing the Integrity of Your ePHI	3/12
Managing Your Media	3/8
Administrative	0/0
Physical	3/7
Technical	0/1
T10	✗
Managing Your Facilities	1/14
Managing Your Workforce	0/9
Educating Your Workforce	0/11
Managing Your Vendors	0/9
Continuing Your Operations When Emergencies Occur	0/20
Auditing Your Operations	0/14
Managing Incidents	0/5

www.HealthIT.gov/security-risk-assessment

Providing Feedback…..



HealthIT.gov › For Providers & Professionals › Privacy & Security › Security Risk Assessment › Comments

Print | Share

Security Risk Assessment

- Integrating Privacy & Security Into Your Medical Practice
- Health Information Privacy and Security: A 10 Step Plan
- Health IT Privacy and Security Resources
- Mobile Device Privacy and Security
- Model Notices of Privacy Practices
- Patient Consent for eHIE
- Privacy & Security Training Games
- Security Risk Assessment
  - Security Risk Assessment Tool

Comments

How can I provide comments?

ONC is asking users to provide comments regarding their use of the Security Risk Assessment (SRA) Tool. These comments will be used to improve future versions of the SRA Tool.

Comments will be accepted from Friday, March 28th to Monday, June 2nd.

[*] denotes required fields

Security Risk Assessment Tool Web Event

It's been about a month since HHS released the Security Risk Assessment (SRA) Tool on March 28th of this year. Since then ONC has received many suggestions, comments and questions . This webinar is designed to review the current state of the tool, discuss some of the known issues and ONC's plan to address those identified issues and answer questions from users across the country.

ONC is looking forward to hearing from the SRA Tool's user community.

Register here and join us at – on April 29th 2014 from 2 – 3:30 pm EDT.

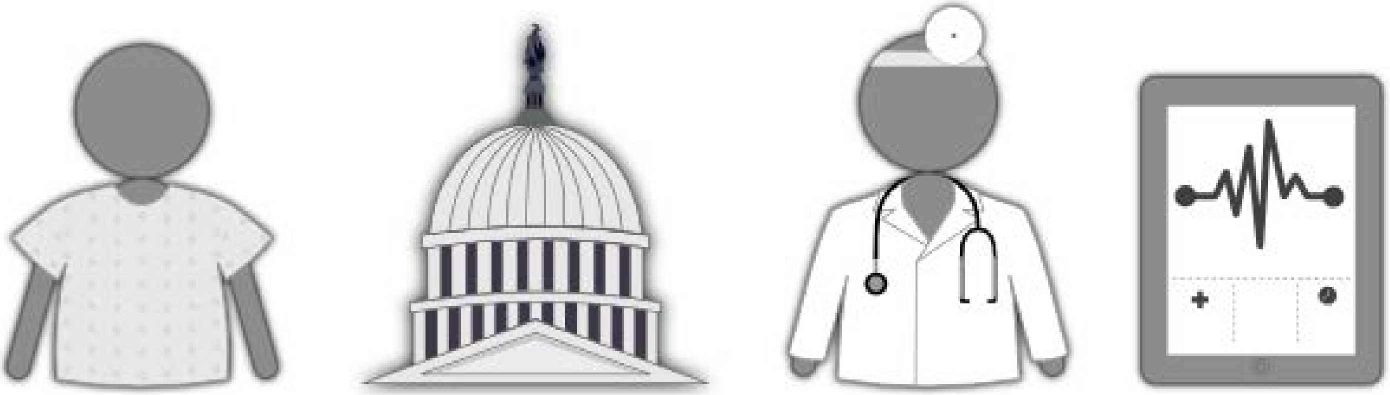
First and Last Name

www.HealthIT.gov/providers-professionals/security-risk-assessment-tool-comments

Feedback Review

- Risk Assessment versus Risk Analysis
- Windows 8.1 download issues
- Unknown publisher/digital certificate issue
- More context on likelihood and impact
- No Mac version or other platforms
- Language is unclear
- X issue on glossary
- Needs Multi-site functionality

We’re All In This Together



Everyone has a role in protecting and securing health information

Download the Full Infographic Today!

HealthIT.gov

HealthIT.gov

Privacy and Security in Health IT

The Office of the National Coordinator for Health IT (ONC) is dedicated to improving the privacy and security of health information

Protecting Health Information: A Shared Responsibility

Health Care Providers
- Understand Rules
- Protect and Secure Information
- Educate Staff and Patients

Government
- Promote Trust
- Develop Policies
- Fairly Enforce Rules

Patients
- Understand Rights
- Protect Personal Information
- Be Engaged

Technology Vendors
- Embrace Privacy by Design
- Provide Convenient Technology
- Implement Standards

ONC Goal: Inspire Confidence And Trust

Promote the Secure Use of Health IT

Information Assurance

Coordinate Development of Privacy and Security Policy

Patient Direct Access to Lab Report (CLIA)

Meaningful Use

Educate and Empower Patients and Providers

Improved Access to Health Information

View and Download Health Records

Patient Education

Enhanced Understanding of Patients

Provide Technical Assistance

Interactive Security Training

Data Segmentation for Privacy

Notice of Privacy Practices

eConsent Trial

HITPC's Privacy & Security Tiger Team Advises ONC

HITPC's Privacy & Security Tiger Team makes recommendations based on Fair Information Practice Principles

extensive public outreach

7 public meetings conducted over a 3-year period

collaboration with stakeholders

and coordination with ONC and other government agencies

Privacy & Security Tiger Team Recommendations To Date

From 2010-2013, the Tiger Team developed 160 recommendations for improving privacy and security of health information.

HITPC forwarded 154 recommendations to ONC

As of September 30, 2013:

ONC has acted upon 133 of the 154 recommendations

53% Fully or Partially Adopted | 33% In Process | 14% Action Pending

We're All In This Together

Everyone has a role in protecting and securing health information

http://www.healthit.gov/policy-researchers-implementers/everyone-has-role-protecting-and-securing-health-information

MANILA
Consulting Group, Inc.

PDF VPAT

Document Information

Document Name/URL:	
Auditor Name:	
Audit Date:	
Authorization Date:	
Authorization Name/Signature:	

	Total remediation Time
Hours	

Requirements Checklist

The following checklist should be used by MANILA staff to verify that PDF documents meet the requirements established by the MANILA 508 Team. The checklist includes compliance with Section 508, in addition to other MANILA requirements. It is intended to be used as a guideline for documents that have an expectation of being published to the web, made available to the general public, or being converted into accessible .pdf files. This template incorporates elements necessary for that conversion to be successful.

ID	1.0 Document Layout and Formatting Requirement	Pass	Fail	N/A
1.1	Does the document contain the necessary Document Property Tags: TITLE, AUTHOR, SUBJECT, KEYWORDS			
1.2	Does the document have the language specified in the Document Property tags?			
1.3	Does the document have a logical reading order, i.e. is this tab order correct?			
1.4	Does the file contain well placed bookmarks that mark pertinent points in the document?			
1.5	Do all URL's contain the correct hyperlinks and display the fully qualified URL (i.e., http://www.manilaconsulting.net and not www.manilaconsulting.net)?			
1.6	If color is used to emphasize the importance of selected text, is there an alternate method?			
1.7	Are all URL's linked to the correct Web destinations?			

ID	1.0 Document Layout and Formatting Requirement	Pass	Fail	N/A
1.8	Have comments been removed and formatting marks been turned off?			
1.9	Have Acrobat Accessibility Tags been added to the document?			
1.10	Has a full Accessibility Report been run on the document in Adobe Acrobat Professional 8 or higher showing no errors are present?			
1.11	Have documents with multi-column text, tables, or call-out boxes been checked for correct reading order using a screen reader?			
1.12	Has a separate accessible version of the document been provided when there is no other way to make the content accessible? (Example: An organizational chart)			
1.13	Has the document been successfully navigated and read with a screen reader (i.e. JAWS)?			

ID	2.0 Document Image Requirement	Pass	Fail	N/A
2.1	Do all images, grouped images and non-text elements that convey information have alternative text descriptions?			
2.2	Is the document absent of scanned images of text?			
2.3	Do complex images have descriptive text immediately after the image?			
2.4	Are multiple associated images on the same page (e.g., boxes in an organizational chart) grouped as one object?			
2.5	Have all multi-layered objects been flattened into one image and use one Alternative Text (Alt Tag) for this image?			

ID	3.0 Document Table Requirements	Pass	Fail	N/A
3.1	Do all data tables in the document have Row and Column headers?			
3.2	Are tables being used to create a tabular structure (not tabs or spaces)?			
3.3	Do all data tables in the document have a logical reading order from left to right, top to bottom?			
3.4	Are data cells in the tables logically associated with the Row/Column Header Elements? Are ID tags used to associate data and header cells for data tables that have two or more logical levels of row or column headers?			
3.5	Are all data tables in the document named, numbered (if applicable) and have a description?			
3.6	Are all table cells, with the exception of those associated with the Header Row, designated as data cells?			

ID	Notes/Additional Requirements	Pass	Fail	N/A
A	Has a visual check been performed on the document to ensure that no hidden data from Word (or other applications used to create the original document) is present in the PDF file?			
B	Does the document file name not contain spaces or special characters?			
C	Is the document file name concise, generally be limited to 20-30 characters, and make the content of the file clear in the context in which it is presented?			
D	The document does not contain scanned signatures?			
E	Does the document utilize embedded or common fonts i.e. Times New Roman, Verdana, Arial, Tahoma and Helvetica?			

Non-Compliant Element Tracking

The following table should be used to document any elements of the asset that failed or were identified as being non-compliant. Identify each failed/non-compliant element of the asset by ID Number and include a description of the reason why the element failed or is non-compliant.

ID	Description of Failure/Non-Compliance

Requirement Guidelines

The following guidelines have been established for PDF files by MANILA Consulting Group Inc. to meet Section 508 Compliance requirements.

1.0 Document Layout and Formatting

1.1. The document should be properly tagged, i.e. the Document Properties / Description tab should have "Yes" selected for "Tagged PDF".

1.2. The document language should be specified, i.e. the Document Properties / Advanced tab should have the Language set to "English", "English US", or possibly "Spanish".

1.3. The document should have a logical reading order, i.e. the Tab Order must be in the correct order to make the document readable.

1.4. If the document contains a Table of Contents (TOC) or Bookmarks they must be functioning correctly.

1.5. All URL's must contain the correct hyperlink and display the fully qualified URL (i.e., http://www.manilaconsulting.net and not www.manilaconsulting.net).

1.6. All URLs must be linked to an active Web Destination.

1.7. All Acrobat Comment and Markup items must be removed from the document. The presence of Comment and Markup items will adversely affect the screen reader's ability to correctly interpret the document.

1.8. All Acrobat Accessibility Tags must be applied to the document. Acrobat Accessibility Tags are added to the document as part of the conversion process and should be visually verified.

1.9. A Full Accessibility Report must be run on the document (using Adobe Acrobat Professional 8 or higher) showing that no errors are present.

1.10. Documents that contain multi-column text, tables, or call-out boxes (i.e. balloons or other graphics with enclosed text) should be checked for correct reading order using the Acrobat Pro 'Read Aloud' function. Using the "Read Aloud" function will also validate that the tab order of the document is correct and that a screen reader will be able to track the correct flow of the document.

1.11. Any document that is unable to be made accessible will need to have a separate accessible version available for disabled users to access. (Example: An organizational chart)

1.12 The entire document must be navigated and read successfully with a screen reader, and the information contained in the document must be able to be identified and deciphered accurately by Assistive Technology.

2.0 Document Images

2.1. All document images, grouped images or non-text elements (charts and graphics) should have Alternative Text (Alt Text) associated with them.

2.2. Documents comprised of scanned images of text are not 508 compliant. Scanned images of text are unable to be accurately interpreted by screen readers and cannot be made compliant. One alternative is to use Adobe Acrobat to rescan the document to text with OCR activated.

2.3. Complex images (i.e. charts, graphs, flowcharts, etc.) must have descriptive text immediately after the image.

2.4. Multiple associated images must be grouped as one object. Grouping the images together will deflect possible errors when the document is presented by the screen reader.

2.5. All multi-layered objects must be flattened into one image and use one Alternative Text (Alt Tag) for this image.

3.0 Document Tables

3.1. Documents containing data tables should have readily identifiable row and column headers.

3.2. Tables should be used to organize information into a tabular format. The use of tabs or spaces to create tabular data will adversely affect the screen reader and should not be used.

3.3. Data tables should have a logical reading order from left to right and top to bottom. This is the table structure that screen readers are designed to follow and any other format will adversely affect its ability to correctly convey the information.

3.4. Table cells should be logically associated with the Row/Column Header i.e. there should be a logical, one-to-one association from the data to the information in the Row/Column Header.

3.5. Tables should be named, have a table number (if applicable) and a have a description. This will allow the screen reader to identify each table and allow the user to recognize the information being presented.

3.6. All cells within a data table, that are not part of the header row, must be designated as "data cells".

Notes/Additional Requirements

A. A visual check should be done to the document to ensure that no hidden data from Word (or other applications used to create the original document) is present in the resulting PDF file.

B. The document file name must not contain spaces or special characters (!,;:?{}@/\=+parentheses?

C. The document file name must be concise, generally be limited to 20-30 characters, to make the content of the file clear in the context in which it is presented.

D. Scanned signatures within documents are a considered a theft-of-identity risk and should not be used. Alternative methods of "signing" documents should be used.